IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application: **Bleizeffer et al.**	§	
	§	
Serial No.: **09/877,157**	§	Group Art Unit: **3621**
	§	
Filed: **June 8, 2001**	§	Examiner: **Winter, John M.**
	§	
For: **Interface for Creating Privacy Policies for the P3P Specification**	§	Attorney Docket No.: **RSW920000172US1**
	§	

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on January 19, 2006.

By: Dell Whitton
Dell Whitton

RESPONSE TO NOTICE OF NON-COMPLIANT AMENDMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Non-Compliant Amendment was received by Applicant stating that "The Appeal Brief filed on June 28, 2005 is defective for failure to comply with one or more provisions of 37 CFR 41.37". A copy of the Notice of Non-Compliant Amendment is attached hereto.

No fees are believed to be necessary. If, however, any fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0461. No extension of time is believed to be necessary. If, however, any fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0461.

In response to the Notice of Non-Compliant Amendment, attached hereto is a copy of the Appeal Brief as filed on January 31, 2005, which includes the Evidence Appendix (including Appendix A, Appendix B and Appendix C) starting at page 27 of 35, and the Related Proceedings Appendix at page 35 of 35. The Appeal Brief was thus filed in accordance with all provisions of 37 C.F.R. 41.37. Also attached is a copy of the PTO Auto-Reply Facsimile Transmission showing receipt of 35 pages of the Appeal Brief as-filed.

As evidenced by the attached printout from the USPTO Patent Application Information Retrieval system (PAIR), the Appeal Brief as filed on January 31, 2005, was improperly scanned into PAIR as five (5) individual documents on January 31, 2005, including:

Document Description	Page Count	(Documents contained)
Appeal Brief Filed	27	Fax Cover Sheet (page 1)
		Transmittal Document (page 2)
		Appeal Brief (pages 3-26)
		Evidence Appendix (page 27)
Appendix to Specification	5	Appendix A (pages 28–31)
		1 page inserted by IFW (no page number)
Appendix to Specification	2	Appendix B (page 32)
		1 page inserted by IFW (no page number)
Appendix to Specification	4	Appendix C (pages 33-34)
		Related Proceedings Appendix (page 35)
		1 page inserted by IFW (no page number)
Fee Worksheet (PTO-875)	1	Transmittal Document (page 2)
		(also included in above "Appeal Brief filed")

The alleged error appears to have actually occurred in the transmission of the Appeal Brief without the attached appendices to the Board of Patent Appeals and Interferences, who stated in the Order Returning Undocketed Appeal to Examiner dated November 3, 2005, that: "A review of the file reveals that the heading "Related Proceedings Appendix" is missing from the Appeal Brief according to §41.37 © (1) (x)". As shown above, the Related Proceedings Appendix was included and received at the USPTO on January 31, 2005.

REMARKS

As shown by Applicants, all provisions under §41.37 have been complied with in the Appeal Brief filed on January 31, 2005. Applicants respectfully request that the Appeal Brief as filed be forwarded in its entirety to the Board of Patent Appeals and Interferences for consideration.

Date: January 19, 2006

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
Wayne Bailey
Registration No. 34, 289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner John M. Winter** **Group Art Unit 3621**	Facsimile No.: **703/872-9306**
From: Carrie Parker Legal Assistant to Wayne Bailey	No. of Pages Including Cover Sheet: **35**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. **09/877,157**
Attorney Docket No: **RSW920000172US1**

Date: Monday, January 31, 2005

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Bleizeffer et al.**

Serial No.: **09/877,157**

Filed: **June 8, 2001**

For: **Interface for Creating Privacy Policies for the P3P Specification**

§ Group Art Unit: **3621**

§ Examiner: **Winter, John M.**

§ Attorney Docket No.: **RSW920000172US1**

§

36736
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on January 31, 2005.
By: Carrie Parker
Carrie Parker

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0461.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

Docket No. RSW920000172US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Bleizeffer et al.**	§	
	§	Group Art Unit: **3621**
Serial No. **09/877,157**	§	
	§	Examiner: **Winter, John M.**
Filed: **June 8, 2001**	§	
	§	
For: **Interface for Creating Privacy Policies for the P3P Specification**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on January 31, 2005.

By: Carrie Parker
Carrie Parker

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on November 30, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-24

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-24
4. Claims allowed: none
5. Claims rejected: 1-24

C. CLAIMS ON APPEAL

The claims on appeal are: 1-24

STATUS OF AMENDMENTS

An amendment after final was filed by Appellants on November 2, 2004, and such amendment was not entered by the Examiner.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

The present invention of Claim 1 is generally directed to facilitating the creation of privacy policies in a data processing system. Through a synergistic combination of data elements, groups and privacy policies, the present invention greatly improves and better facilities a user's ability to define/edit privacy policies when compared to prior privacy techniques which required detailed and extensive user interviews to establish a user's privacy requirements. The data processing apparatus-implemented method is particular advantageous in facilitating an improved user interface for creating privacy policies in a data processing system.

Specifically, Claim 1 is directed to a data processing apparatus-implemented method for creating a privacy policy. A policy group is created (Specification page 19, lines 2-6; Figure 7, step 714). A data element is moved to the policy group (Specification page 19, lines 10-22; Figure 7, step 718). A privacy policy is generated based upon the policy group (Specification page 21, lines 1-15; Figure 7, step 710 and Figure 8, steps 810-824).

B. CLAIM 12 - INDEPENDENT

Claim 12 is directed to an apparatus for creating a privacy policy. The apparatus comprises creation means for creating a policy group (Specification page 19, lines 2-6; Figure 7, step 714, with corresponding structure shown at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300), movement means for moving a data element to the policy group (Specification page 19, lines 10-22; Figure 7, step 718, with corresponding structure shown at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300), and generation means for generating a privacy policy based on the policy group (Specification page 21, lines 1-15; Figure 7, step 710 and Figure 8, steps 810-824, with corresponding structure shown at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300).

C. CLAIM 23 - INDEPENDENT

The present invention of Claim 23 provides an improved user-interface to facilitate co-action with a user for creating a privacy policy. Three distinct portions of the user interface synergistically co-act with the user and with one another to provide such improved user-interface, where information in one portion of the user-interface is used when generating information pertaining to other of the portions of the user interface.

Specifically, Claim 23 is directed to an interface for creating a privacy policy. The interface includes (i) a first portion for displaying predefined data elements (Specification page 11, line 29 – page 12, line 7; Figure 4, element 410), (ii) a second portion for displaying groups of data elements, wherein a group of data elements shares at least one common property (Specification page 12, lines 8-16; Figure 4, element 420), and (iii) a third portion for displaying a privacy policy generated from the groups of data elements (Specification page 12, lines 17-29; Figure 4, element 430).

D. CLAIM 24 - INDEPENDENT

Claim 24 is directed to a computer program product, in a computer readable medium, for creating a privacy policy. The computer program product comprises instructions for creating a policy group (Specification page 19, lines 2-6; Figure 7, step 714), instructions for moving a data element to the policy group (Specification page 19, lines 10-22; Figure 7, step 718), and instructions for generating a privacy policy based on the policy group (Specification page 21, lines 1-15; Figure 7, step 710 and Figure 8, steps 810-824).

E. CLAIM 15 – DEPENDENT MEANS-PLUS-FUNCTION

The corresponding structure for the claimed functions recited in Claim 15 is shown to be at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300.

F. CLAIM 16 – DEPENDENT MEANS-PLUS-FUNCTION

The corresponding structure for the claimed functions recited in Claim 16 is shown to be at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300.

G. CLAIM 17 – DEPENDENT MEANS-PLUS-FUNCTION

The corresponding structure for the claimed functions recited in Claim 17 is shown to be at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300.

H. CLAIM 18 – DEPENDENT MEANS-PLUS-FUNCTION

The corresponding structure for the claimed functions recited in Claim 18 is shown to be at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300.

I. CLAIM 21 – DEPENDENT MEANS-PLUS-FUNCTION

The corresponding structure for the claimed functions recited in Claim 21 is shown to be at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300.

J. CLAIM 22 – DEPENDENT MEANS-PLUS-FUNCTION

The corresponding structure for the claimed functions recited in Claim 22 is shown to be at Figure 1, elements 104, 108, 110 and 112, Figure 2, element 200, and Figure 3, element 300.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-22)

Claims 1-22 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

B. GROUND OF REJECTION 2 (Claims 1-24)

Claims 1-24 stand rejected under 35 U.S.C. § 103 as being unpatentable over Moriconi et al (US Patent 6,158,010) in view of Abraham et al (WO 98/40987).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-22)

The Examiner rejected Claims 1-22 under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. This rejection is respectfully traversed.

A.1. Claims 1-11

Claim 1 specifically recites a data processing apparatus-implemented method, and the recited steps are data processing apparatus-implemented steps. Contrary to the Examiner's statement that Claim 1 "only recites an abstract idea" and "This process might be performed without the aid of any technology and therefore the claimed method is not within the technological arts", Appellants urge that Claim 1 expressly recites technology (a data processing apparatus) and therefore is directed to "useful arts".

Therefore, the Examiner's reasoning in rejecting Claim 1 is shown to be clearly erroneous. In addition, and as shown above, Claim 1 properly recites statutory subject matter pursuant to 35 U.S.C. §101.

With respect to dependent Claims 2-11, Appellants traverse for reasons given above regarding independent Claim 1.

A.2. Claim 12-22

In rejecting Claim 12 in the final Office Action (dated 9/9/2004, last paragraph on page 3 of such Office Action), the Examiner states "In claims 1 and 12 the applicant claims a method for creating policy groups, moving a data element between groups and generating a privacy policy based upon the policy group". Appellants urge that Claim 12 does *not* claim a method. Rather, Claim 12 expressly recites an *apparatus* with corresponding "means for" elements, as shown below:

> 12. An **apparatus** for creating a privacy policy, comprising:
> creation **means for creating** a policy group;

movement **means for moving** a data element to the policy group; and

generation **means for generating** a privacy policy based on the policy group.

Per 35 USC 112, 6th paragraph, "means for" elements shall be construed to cover the corresponding structure or material described in the specification and equivalents thereof. Thus, the recited means for elements are shown to not merely describe a process that might be performed without the aid of any technology, as alleged by the Examiner. Therefore, the Examiner's reasoning regarding Claim 12 in finally rejecting such claim under 35 USC 101 is shown to be clear error, as such claim does not merely recite a method or an abstract idea, as alleged by the Examiner, but rather explicitly recites an apparatus. Claim 12 is thus shown to have been erroneously rejected under 35 U.S.C. § 101.

With respect to dependent Claims 13-22, Appellants traverse for reasons given above regarding independent Claim 12.

B. GROUND OF REJECTION 2 (Claims 1-24)

B.1. Claim 1 (and Claims 12 and 24)

In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. Id. To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03 (emphasis added by Appellants). *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Appellants will now show that all of the claim limitations are not taught or suggested by the cited references.

(i). Generally speaking, the present invention is directed to *privacy policies*, and in particular to methods and apparatus for creating a *privacy policy*. None of the cited references teach or

suggest any type of privacy policy, or the creation of a privacy policy.

Specifically with respect to Claim 1, such claim recites a data processing apparatus-implemented method for creating a *privacy policy*. In contrast, the teachings in the cited Moriconi reference are directed to ensuring that clients are authorized to access securable components (Col. 13, lines 14-32) by use of a *security policy* (Claim 1). Security and privacy are two very different concepts, and the teaching of one (security, as taught by Moriconi) does not teach or suggest the other (privacy, as claimed). For example, imagine a person living in a locked, bullet-proof glass house, where the glass is see-through. This locked, bullet-proof glass house is certainly secure, but it is not at all private. As another example, assume that an ID is required to authenticate that a user is who they are in order to receive a ballot for voting. However, the ballot itself has the user's name/identifier on it. The user has been authorized to vote, but the voting is certainly not private as the voter's name is in the ballot. Thus, authorization and privacy shown to be very different concepts, as will now be further described (with supporting evidence), and a teaching of one (security) does not teach or otherwise suggest the other (privacy).

The following is an excerpt from a document entitled "Authorization and Privacy for Semantic Web Services", published by IEEE Distributed Online Systems, which is from the July/Aug 2004 issue of IEEE Intelligent systems. The document, which is attached hereto in Appendix A, was found by Appellants on the internet at http://dsonline.computer.org/0410/f/x4kag.htm.

Role of policies

Policies specify who can use a service and under which conditions, how information should be provided to the service, and how the provided information will be used. Policies should be part of Web Service representations—particularly those on the Semantic Web (see the "Related Work" sidebar for more background information).

In our work, a client-server model involves a client that wants to invoke a Web Service. We view the use of policies as *symmetric*—policies that constrain both the provider and requester. You can easily extend this model to a service-service architectural model.

Here, we address two kinds of policies: *privacy* and *authorization*. Privacy policies specify under what conditions you can exchange information and the legitimate uses of that information. For example, a privacy policy might say that a provider could give a requester a key to access private information only if the key is encrypted during

> transmission. When a requester discovers the policy, it should decide whether it can satisfy this condition. The requester might have its own privacy policy that requires keeping certain information confidential, so it likewise can't share unencrypted private information. The requestor's privacy policy prevents it from interacting with Web Services that don't perform the needed encryption.
>
> Privacy policies help specify data confidentiality during transmission as well as after receipt. Consider a service that says it won't distribute details it receives as input. A requester that values privacy might see this as an important requirement.
>
> You can interpret a Web Service's privacy policies as an obligation and contract. For example, if after invocation, a service does provide a requester's details to a telemarketer, the person represented by the requester could take legal action against the service on the basis of the policy. As financial transactions become more common among Web Services and as Web Services start dealing with confidential information (such as names, addresses, social security numbers (SSNs), credit cards, and telephone numbers), more people will expect the enforcement of privacy policies.
>
> Authorization policies constrain the provider to accept requests for service only from certain clients. For example, a service's authorization policy could state that a requester must act on behalf of a person who belongs to a certain organizational group and can prove membership with a digital certificate. Similarly, the requester could limit invocation to selected providers.

This document clearly shows that authorization policies and privacy policies are not the same, and that one is not a subset of the other. They are different. Appellants urge that a teaching of authorization – as taught by the cited Moriconi reference - does not teach or suggest any type of privacy policy, as claimed.

Also attached hereto in Appendix B is a datasheet from Electronic Data Systems Corporation (EDS) regarding their Security and Privacy Consulting Services. If security and privacy were coextensive, or even if one were a subset of the other, there would be no reason to include both terms in the title of this document as it would be redundant. Because each term is used in the title further evidences that one does not mean, or otherwise include/cover, the other.

Thus, per the technological arts, authorization/security policies and privacy policies are different, and a teaching of one does not teach or suggest the other.

Even in the non-technological arts, it is commonly known that in today's environment with terrorists-related concerns, people everywhere are having to make trade-offs regarding their own privacy in the name of security (as shown in Appendix C in a document entitled "Trading

Privacy for Security Without a Thought", by Ellen Goodman and posted at www.siliconvalley.com on Oct. 6, 2002). This further evidences that these terms (security and privacy) mean different things to those of ordinary skill in the art, and thus a teaching of one (security policy) does not teach or otherwise suggest the other (privacy policy).

Therefore, it is shown that the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 1, as the cited reference does not teach or otherwise suggest any type of method for creating a privacy policy, or any step of *creating* a privacy policy based on a policy group, as expressly recited in Claim 1.

(ii). The Examiner takes the position that an authorization policy "by definition" is also enforcing a privacy policy. Appellants show two-fold error in such assertion. First, an authorization policy does *not*, by definition, also enforce a privacy policy. The Examiner provides no evidence whatsoever to substantiate such assertion, but rather makes a single sentence unsubstantiated assertion. Appellants have provided ample evidence (above) that an authorization policy is different from a privacy policy, and therefore an authorization policy does not, by definition, also enforce a privacy policy.

Even assuming arguendo that an authorization policy does also enforce a privacy policy (which Appellants urge it does not), Claim 1 is not directed to *enforcement* of a privacy policy. Rather, Claim 1 is directed to the establishment or *creation* of a privacy policy. By analogy, legislatures make laws which the police enforce. Enforcement of laws (by the police) is very different from the process of establishing laws (by legislatures). Similarly, the Examiner's position that a teaching of an authorization policy "by definition" also *enforces* a privacy policy does not establish any teaching or suggestion of any step, process or method for *creating* a privacy policy, as expressly recited in Claim 1. Therefore, even assuming arguendo that the Examiner's assertion regarding authorization and privacy is true (which Appellants urge it is not), the Examiner has still failed to establish a prima facie showing of obviousness as the Examiner has failed to establish any teaching or suggestion of *creating* a privacy policy, or any step of creating a privacy policy *based on a policy group*. Thus, Claim 1 is further shown to have been erroneously rejected Claim 1 under 35 USC § 103.

(iii). Quite simply, a teaching of creating an authorization/security policy does not teach or otherwise suggest any type of privacy policy, and in particular does not teach or suggest a method for creating a privacy policy, or any step of creating a privacy policy based on a policy group, as expressly recited in Claim 1. Thus, A prima facie case of obviousness has not been established by the Examiner with respect to Claim 1, and therefore Claim 1 is shown to have been erroneously rejected.

B.2. Claim 4 (and Claim 15)

Appellants further show error in the rejection of dependent Claim 4, as none of the cited references teach or otherwise suggest the claimed steps of updating a policy-wide property, and generating the privacy policy based on the policy-wide property. In rejecting Claim 4, the Examiner states that Moriconi teaches both of these claimed steps at column 5, lines 48-55. Appellants urge that there, Moriconi states:

> "The present invention includes a system and method for **managing** and **enforcing** complex security requirements in a distributed computer network, and comprises a policy manager located on a server for **managing** and **distributing** a policy to a client, and an application guard located on the client, the application guard acting to **grant or deny access** to various components of the client, as specified by the policy." (emphasis added by Appellants)

As can be seen, this passage generally describes an ability to "manage" and "enforce" security requirements, including a policy manager for "managing" and "distributing" a policy to a client and an application guard that can "grant" or "deny" access to various client components as "specified" by a policy. This passage does not teach or otherwise suggest any step of "updating a policy-wide property" or "generating the privacy policy based on the policy-wide property", as expressly recited in Claim 4. Therefore, the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 4, and accordingly the burden has not shifted to

Appellants to rebut an obviousness assertion. In addition, as the Examiner has failed to properly establish a prima facie showing of obviousness, Claim 4 is shown to have been erroneously rejected pursuant to *In re Fine*, supra.

B.3. Claim 5 (and Claim 16)

With respect to Claim 5, Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein the step of generating a privacy policy comprises generating a human-readable version of the policy". The Examiner states that although Moriconi does not expressly teach this claimed step, "it would be obvious that if the policy is manipulated via a GUI it would be readable to a user". Appellants urge that to the contrary, Moriconi teaches that policy rules developed at policy manager 210 are compiled into an optimized form before being distributed to target application guards (col. 11, lines 21-26). There is no teaching or suggestion that this optimized and compiled form is human-readable. The fact that a prior art device could be modified so as to produce the claimed device is not a basis for an obviousness rejection unless the prior art suggested the desirability of such a modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). The cited reference does not suggest any desire to modify the teachings contained therein to generate a human-readable version of the policy as a part of generating a privacy policy based on a policy group. Hence, it is shown that the Examiner's assertion that this missing claimed feature would have been obvious is not well founded in law or in fact, and thus Claim 5 has been erroneously rejected.

B.4. Claims 6 and 7 (and Claims 17 and 18)

With respect to Claims 6 and 7, Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein the human-readable version of the policy comprises a hypertext markup language version of the policy" (Claim 6), or "wherein the step of generating a privacy policy comprises generating an extensible markup language version of the policy" (Claim 7). The Examiner states that these claimed features are "well-known" and thus "obvious". Appellants show error in such "well-known" basis for rejection. As stated by the Federal Circuit, "virtually all [inventions] are combinations of old elements." *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 698, 218 USPQ 865, 870 (Fed. Cir. 1983); *see also Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1579-80, 219 USPQ 8, 12 (Fed. Cir. 1983) ("Most, if not all, inventions are

combinations and mostly of old elements."). Therefore an examiner may often find every element of a claimed invention in the prior art. If identification of each claimed element in the prior art were sufficient to negate patentability, very few patents would ever issue. Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to determine patentability." *Sensonics, Inc. v. Aerosonic Corp.*, 81 F.3d 1566, 1570, 38 USPQ2d 1551, 1554 (Fed. Cir. 1996). Thus, the Examiner's assertion that the features of Claims 6 and 7 are well known and thus obvious is shown to be an erroneous basis for making an obviousness rejection.

B.5. Claim 10 (and Claim 21)

Further with respect to Claim 10, Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein the step of generating a privacy policy further comprises generating a table of policy elements, wherein a policy element in the table of policy elements corresponds to the policy statement". In rejecting Claim 10, the Examiner states that the cited Moriconi reference teaches that rules are stored in a database/table at col. 4, lines 34-37. Appellants urge that Claim 10 goes beyond such Examiner assertion. The cited passage merely states that a policy server 'stores' and 'manages' the policy rules in a centrally administered database. In contrast, Claim 10 is a further refinement of Claim 9, and expressly recites a particular correlation between the information in the table and another item – the policy statement. In particular, Claim 10 states that a policy element in the table of policy elements corresponds to the policy statement (the policy statement being defined in Claim 9 to be "wherein the step of generating a privacy policy comprises generating a policy statement corresponding to the policy group"). The Examiner has not alleged, nor does the cited reference teach or suggest, any step of "generating a table of policy elements, *wherein a policy element in the table of policy elements corresponds to the policy statement*" (emphasis added by Appellants). Therefore, the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 10, and accordingly the burden has not shifted to Appellants to rebut an obviousness assertion. In addition, as the Examiner has failed to properly establish a prima facie showing of obviousness, Claim 10 is shown to have been erroneously rejected pursuant to *In re Fine*, supra.

B.6. Claim 11 (and Claim 22)

Further with respect to Claim 11, Appellants urge that none of the cited references teach or suggest the claimed steps of identifying an error in the privacy policy, and generating an error statement describing the error. As none of the cited references teach or suggest any type of privacy policy, it necessarily follows that the cited references do not teach or suggest any step of identifying an error in such (missing) privacy policy. Further, there is no teaching/suggestion of generating an error statement describing the error. The Examiner acknowledges this teaching deficiency of the cited references, but states that this step is "well-known" and thus obvious. For similar reasons to those described above with respect to Claims 6 and 7, such "well-known" rationale is not a proper basis for making an obviousness rejection. Thus, Claim 11 is further shown to have been erroneously rejected for at least two additional reasons.

B.7. Claim 23

With respect to Claim 23, Appellants urge that none of the cited references teach or suggest an interface for creating a privacy policy, comprising a first portion for displaying predefined data elements, a second portion for displaying groups of data elements, wherein a group of data elements shares at least one common property, and a third portion for displaying a privacy policy generated from the groups of data elements. In rejecting Claim 23, the Examiner states that Moriconi teaches an interface comprising a first portion for displaying predefined data elements at col. 9, lines 45-50, and a second portion for displaying groups of data elements at Figure 4. Appellants urge that while the cited passage at col. 9 mentions a graphical user interface, it generally describes such interface as providing a user-friendly set of menu options or management services to fully "operate" the policy manager. Moriconi Figure 4 does not describe any specific aspect of a user interface. In contrast, the first two claimed features of Claim 23 specifically recite an interface having two distinct portions – a first portion (for displaying predefined data elements) and a second portion (for displaying groups of data elements). Contrary to the Examiner's assertion, the cited Moriconi reference does not teach or otherwise suggest an interface having these two specific portions.

Still further with respect to Claim 23, the Examiner acknowledges that the cited Moriconi reference does not teach an interface having a third portion for displaying a privacy policy

generated from the groups of data elements, but states that the cited Abraham reference teaches this claimed third portion in the Abstract. Appellants urge that this cited Abraham passage merely states that a graphical user interface is provided such that an operator can input (1) vital information, (2) mapping information, and (3) policies. Appellants urge that a teaching of providing a graphical user input that allows a user to input various information does not teach or otherwise suggest specific details of the interface, and in particular does not teach or otherwise suggest an interface having a third portion for *displaying a privacy policy generated from the groups of data elements*. Therefore, the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 23, and accordingly the burden has not shifted to Appellants to rebut an obviousness assertion. In addition, as the Examiner has failed to properly establish a prima facie showing of obviousness, Claim 23 is shown to have been erroneously rejected pursuant to *In re Fine*, supra.

Finally, even when combining the teachings of the two cited references, there is still no teaching or suggestion of an interface having three distinct portions – a first portion (for displaying predefined data elements), a second portion (for displaying groups of data elements), and a third portion (for displaying a privacy policy *generated from* the groups of data elements). This further evidences that Claim 23 has been erroneously rejected under 35 U.S.C. § 103, as all claimed features are not taught or suggested by the cited references.

In conclusion, all claims recite statutory subject matter. In addition, none of the cited references teach or otherwise suggest any type of *privacy policy*, and in particular the cited references do not teach or suggest a method for *creating* a privacy policy, or any step of creating a privacy policy *based on a policy group*. Thus, a prima facie case of obviousness has not been established by the Examiner, and therefore all claims are shown to have been erroneously rejected. Accordingly, Appellants urge that the rejection of such claims be reversed by the Board.

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A data processing apparatus-implemented method for creating a privacy policy, comprising data processing apparatus-implemented steps of:

creating a policy group;

moving a data element to the policy group; and

generating a privacy policy based on the policy group.

2. The method of claim 1, wherein the data element is a predefined data element.

3. The method of claim 1, wherein the data element comprises at least one sub-element.

4. The method of claim 1, further comprising:

updating a policy-wide property; and

generating the privacy policy based on the policy-wide property.

5. The method of claim 1, wherein the step of generating a privacy policy comprises generating a human-readable version of the policy.

6. The method of claim 5, wherein the human-readable version of the policy comprises a hypertext markup language version of the policy.

7. The method of claim 1, wherein the step of generating a privacy policy comprises generating an extensible markup language version of the policy.

8. The method of claim 1, wherein the step of generating a privacy policy comprises generating a compact policy.

9. The method of claim 1, wherein the step of generating a privacy policy comprises generating a policy statement corresponding to the policy group.

10. The method of claim 9, wherein the step of generating a privacy policy further comprises generating a table of policy elements, wherein a policy element in the table of policy elements corresponds to the policy statement.

11. The method of claim 1, further comprising:

identifying an error in the privacy policy; and

generating an error statement describing the error.

12. An apparatus for creating a privacy policy, comprising:

creation means for creating a policy group;

movement means for moving a data element to the policy group; and

generation means for generating a privacy policy based on the policy group.

13. The apparatus of claim 12, wherein the data element is a predefined data element.

14. The apparatus of claim 12, wherein the data element comprises at least one sub-element.

15. The apparatus of claim 12, further comprising:

means for updating a policy-wide property; and

means for generating the privacy policy based on the policy-wide property.

16. The apparatus of claim 12, wherein the generation means comprises means for generating a human-readable version of the policy.

17. The apparatus of claim 16, wherein the human-readable version of the policy comprises a hypertext markup language version of the policy.

18. The apparatus of claim 19, wherein the generation means comprises means for generating an extensible markup language version of the policy.

19. The apparatus of claim 12, wherein the generation means comprises means for generating a compact policy.

20. The apparatus of claim 12, wherein the generation means comprises means for generating a policy statement corresponding to the policy group.

21. The apparatus of claim 20, wherein the generation means further comprises means for generating a table of policy elements, wherein a policy element in the table of policy elements corresponds to the policy statement.

22. The apparatus of claim 12, further comprising:

means for identifying an error in the privacy policy; and

means for generating an error statement describing the error.

23. An interface for creating a privacy policy, comprising:

a first portion for displaying predefined data elements;

a second portion for displaying groups of data elements, wherein a group of data elements shares at least one common property; and

a third portion for displaying a privacy policy generated from the groups of data elements.

24. A computer program product, in a computer readable medium, for creating a privacy policy, comprising:

instructions for creating a policy group;

instructions for moving a data element to the policy group; and

instructions for generating a privacy policy based on the policy group.

EVIDENCE APPENDIX

Evidence Appendix follows.

APPENDIX A

1 of 4

From the Jul./Aug. 2004 issue of *IEEE Intelligent Systems*

IEEE Intelligent Systems

Authorization and Privacy for Semantic Web Services

Lalana Kagal and Tim Finin • University of Maryland
Massimo Paolucci, Naveen Srinivasan, and Katia Sycara • Carnegie Mellon University
Grit Denker • SRI International

Providing guarantees for security and privacy is paramount to the success of Semantic Web Services. In this article, the authors describe OWL-S policy annotations and extend the OWL-S Matchmaker and OWL-S Virtual Machine to support the processing of those policies.

Web Services will soon handle users' private information. They'll need to provide privacy guarantees to prevent this delicate information from ending up in the wrong hands. More generally, Web Services will need to reason about their users' policies that specify who can access private information and under what conditions.

These requirements are even more stringent for Semantic Web Services that exploit the Semantic Web to automate their discovery and interaction because they must autonomously decide what information to exchange and how.

In our previous work, we proposed ontologies for modeling the high-level security requirements and capabilities of Web Services and clients.[1] This modeling helps to match a client's request with appropriate services—those based on security criteria as well as functional descriptions. For example, a Web Service could state that it can perform OpenPGP encryption and requires an invoker that can authenticate itself and communicate in XML. We added functionality to the DAML-S Matchmaker[2] (an earlier version of the OWL-S Matchmaker) that lets it verify if a service's capabilities fulfill the invoker's

security requirements and vice versa. Our results assist coarse-grain matching decisions such as "Does the service provide encryption?" or "What kind of credential do I have to provide to authenticate myself to the service?"

In this article, we propose a more fine-grain security markup of service parameters in OWL-S. We extend our previous work with annotations about the security and privacy policies of services. We express these annotations in Rei, a logic-based language that lets you define rules and constraints over domain-specific ontologies.[3] Our work aims to provide security and policy annotations for OWL-S service descriptions and enforcements by extending the OWL-S Matchmaker for policy matching and the OWL-S Virtual Machine (VM)[4] with policy enforcement and security mechanisms.

next »

Role of policies

Policies specify who can use a service and under which conditions, how information should be provided to the service, and how the provided information will be used. Policies should be part of Web Service representations—particularly those on the Semantic Web (see the "Related Work" sidebar for more background information).

In our work, a client-server model involves a client that wants to invoke a Web Service. We view the use of policies as *symmetric*—policies that constrain both the provider and requester. You can easily extend this model to a service-service architectural model.

Here, we address two kinds of policies: *privacy* and *authorization*. Privacy policies specify under what conditions you can exchange information and the legitimate uses of that information. For example, a privacy policy might say that a provider could give a requester a key to access private information only if the key is encrypted during transmission. When a requester discovers the policy, it should decide whether it can satisfy this condition. The requester might have its own privacy policy that requires keeping certain information confidential, so it likewise can't share unencrypted private information. The requestor's privacy policy prevents it from interacting with Web Services that don't perform the needed encryption.

Privacy policies help specify data confidentiality during transmission as well as after receipt. Consider a service that says it won't distribute details it receives as input. A requester that values privacy might see this as an important requirement.

You can interpret a Web Service's privacy policies as an obligation and contract. For example, if after invocation, a service does provide a requester's details to a telemarketer, the person represented by the requester could take legal action against the service on the basis of the policy. As financial transactions become more common among Web Services and as Web Services start dealing with confidential information (such as names, addresses, social security numbers (SSNs), credit cards, and telephone numbers), more people will expect the enforcement of privacy policies.

Authorization policies constrain the pro-vider to accept requests for service only from certain clients. For example, a service's authorization policy could state that a requester must act on behalf of a person who belongs to a certain organizational group and can prove membership with a digital certificate. Similarly, the requester could limit invocation to selected providers.

A motivating example

Consider a scenario in which a scientist is looking for an online computing service for her experimental data. Her privacy policy requires that any personal information provided to the service (such as name or SSN) stay confidential. So, she's only looking for Web Services that accept encrypted data and that don't release personal information to other services or agents.

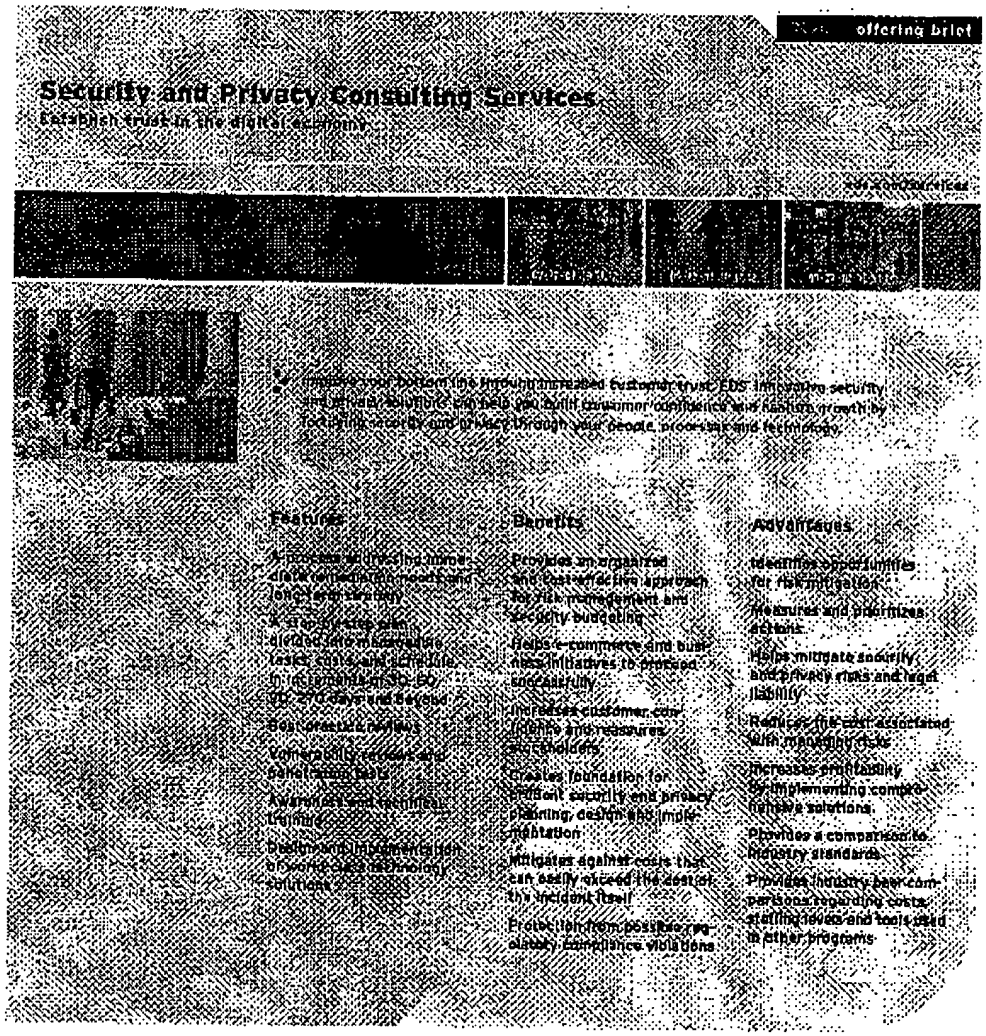
The scientist finds a Web Service that can perform the necessary data computations. The service's authorization policy says that it allows access only to members of certain, selected organizations and that the scientist's registration must be authenticated.

In this article, we'll approach the formalization and processing of these privacy and authentication policies on two abstraction levels. On a more abstract level, we provide ontologies to annotate Web Service input and output parameters with security characteristics that state whether these parameters are encrypted or digitally signed, and we rely on Rei to formalize the privacy and authorization policies.

On a more concrete level, selecting Web Services that satisfy the requester's policies will be part of an extension of the OWL-S matchmaking process. Furthermore, cryptographic mechanisms such as encrypting or signing messages are enforced via integration into the OWL-S VM, a generic processor for the OWL-S process model and tool for automatic invocation of OWL services.

next »

APPENDIX B



offering brief

Security and Privacy Consulting Services

Establish trust in the digital economy

Features

Benefits

Advantages

APPENDIX C

SiliconValley.com

Posted on Sun, Oct. 06, 2002

Trading privacy for security without a thought

By Ellen Goodman

From time to time, my husband and I ask each other a humbling question about the human condition: How would you like to see your 10 worst moments on videotape?

This is the fate that befell Madelyne Toogood last month when she was captured on a security camera in a department store parking lot. The mother was taped slapping around her 4-year-old daughter as they got into their SUV.

Toogood got to see this moment -- which we sincerely *hope* was one of her 10 worst -- again and again and again. The police saw it. The entire nation saw it. Today, the Indiana court where she will be tried for a felony charge of battery will also see it.

Toogood's tape has become the Rodney King tape of child abuse. A debate ensued about parenting and ``spanking,'' about the line between discipline and abuse. The mother's only defense after seeing her self-portrait was to swear, ``I'm not a monster.'' That too was debated.

In fact, the public air was full of heated opinions and judgments about everything . . . except the videotape itself. No one seemed too concerned about the image or its trail from Kohl's to CNN.

We have gotten so used to the idea of a security camera peering at us out of every ATM and parking lot, every airport and school, every department store and public square, that we no longer question it. When the booty of a department store's private eye is open to the public eye, we don't flinch. We just watch.

Indeed, the only story alarming enough to raise privacy hackles these days came from Washington state, where two men were arrested for taking pictures up women's skirts. But these men were acquitted of voyeurism by the state Supreme Court because the pictures were taken in public places where, the justices ruled, people don't have a ``reasonable expectation of privacy.''

It seems that the old expectation of privacy in public has become unreasonable. There are now video cameras in the remote part of a national forest for the stated purpose of catching people growing marijuana. There are at least 2,397 surveillance cameras on the streets of Manhattan.

We've become a nation of surveillance with remarkably little discussion. Few of us are asking the questions offered by David Sobel of the Electronic Privacy Information Center: ``What becomes of any tapes created by such systems, who has access to them and how might they be used?'' Nor are we asking what it means for a nanny or a student or a shopper to be on permanent candid camera.

It sounds old-fashioned to fuss about being watched. The philosopher Jeremy Bentham once described the perfect prison as a ``panopticon'' where prisoners were under complete surveillance and yet could not see the watcher. But that was in the 18th century.

In ``1984,'' the inevitable textbook of Big Brotherhood, George Orwell wrote: ``There was of course no way of knowing whether you were being watched at any given moment. . . . You had to live -- did live,

from habit that became instinct -- in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized." But he wrote that in 1949.

Today people audition to go on ``Big Brother 3." A woman gives birth on the Web. Since Jennifer Ringley ``jennicammed" her way to fame, many others have chosen to live in the public eye, 24/7.

If the threshold of privacy has been lowered, the threshold of anxiety has been heightened. So we accept scrutiny as the price of security.

In this process, we don't always recognize when the camera has become the voyeur. Ads for Web cams pop up over the Internet featuring shadowy images of couples in bed. William Staples, sociologist and author of ``Everyday Surveillance," notes that ``the sell is security but the hook is voyeurism." Meanwhile, one security camera picks up Madelyne Toogood in a ``moment." But another may tape a couple necking in the car or a customer tripping over her feet. Next thing you know your image is out there on the Internet, says Staples.

Frankly, I am comforted by a security camera in a parking garage late at night. And I know that videotapes are useful for police investigations . . . after the crime. But if security is overrated, intrusion may be underrated.

The Toogood reality show ended with a mother in court and a child in foster care and a second debate about whether this did more harm than good. Surely we should spend some of the same energy debating the collective life of the videocammed American? How many little brothers add up to a big one?

Look up there. Is that a security guard watching? Or is it a Peeping Tom?

Ellen Goodman is a Boston Globe columnist.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.